

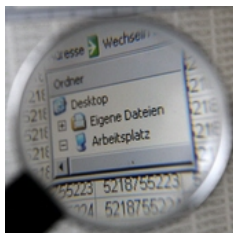
21.09.2009, 10:08 Uhr

## Wirtschaftskriminalität

### Betriebsspione nehmen Mittelständler ins Visier

von Carmen Salvenmoser

**Industriespitzel haben es längst nicht mehr nur auf Konzerne abgesehen. Sie spähen auch mittelständischen Unternehmen im Auftrag der Konkurrenz aus und stehlen sensible Daten. Die Komplizen der Spione kommen häufig aus den eigenen Reihen.**



Nicht nur Großunternehmen werden Opfer von Betriebsspionen. Quelle: dpa

KÖLN HB. Eginhard Vietz kann ein Lied von Betriebsspionen singen. Der US-Geheimdienst CIA hackte sich in das Computersystem des Mittelständlers, um an Geschäftsdaten zu kommen, behauptet der Geschäftsführer des niedersächsischen Pipelinebauers Vietz GmbH. Und ein chinesischer Staatsbetrieb kupferte gleich eine komplette Produktionsanlage ab.

Wie Vietz geht es vielen Mittelständlern. Entgegen des verbreiteten Irrglaubens, nur Großunternehmen würden Betriebsspionen zum Opfer fallen, sind auch Mittelständler beliebte Zielscheiben von wissbegierigen Konkurrenten: "Die Opfer haben innovative Produkte und sind in vielen Bereichen heimlicher Weltmarktführer", sagt Christian Schaaf, Geschäftsführer der Münchener Sicherheitsberatung Corporate Trust. Dadurch gerieten auch Mittelständler ins Visier von Spitzeln konkurrierender Unternehmen, und sogar ausländische Geheimdienste spähen im Dienste der eigenen Wirtschaft deutsche Firmen aus. Industriespionage ist laut Schaaf heute gängige Praxis.

Im Gegensatz zu großen Konzernen seien die meisten Mittelständler aber nicht ausreichend auf die Gefahr vorbereitet, warnt der Experte: "Fast alle Großunternehmen haben eine Sicherheitsabteilung als Schutzschild. Mittelständische Firmen sind hingegen meist nicht auf Angriffe gefasst."

Das mag auch daran liegen, dass viele Unternehmen nicht ausreichend über Wirtschaftskriminalität Bescheid wissen. "Genau deshalb unterschätzen sie das Risiko, selbst Opfer zu werden und investieren zu wenig in die Prävention", sagt Jörg Ziercke, Präsident des Bundeskriminalamts. Das bestätigt auch die Studie "Industriespionage" von Corporate Trust: Obwohl über 80 Prozent der Befragten glauben, dass das Risiko für Industriespionage weltweit ansteigen wird, glauben nur knapp 34 Prozent, dass die Gefahr auch für das eigene Unternehmen steigen wird.

Zu einem alarmierenden Ergebnis kommt auch eine aktuelle Umfrage des Arbeitskreises Sicherheit in der Wirtschaft (ASW). 40 Prozent der befragten Firmen gaben an, in den vergangenen zwei Jahren ausspioniert worden zu sein. Schäden von mindestens 2,8 Milliarden Euro sind der deutschen Wirtschaft dadurch entstanden, der Hamburger Verfassungsschutz schätzt die Dunkelziffer sogar auf 50 Milliarden Euro. Besonders gefährdet sind laut Sicherheitsexperte Schaaf technologiegetriebene Branchen wie der Maschinenbau, die Nanotechnologie oder die Energiewirtschaft.

Spitzel versuchen meist, technische Innovationen und Produktionsabläufe auszuspähen oder Vertriebskanäle, Kundendaten und Margen in Erfahrung zu bringen. Und bedienen sich dabei oft einfacher Methoden: Das Aushorchen argloser Mitarbeiter mit ein paar geschickten Fragen oder das Abhören von vertraulichen Gesprächen gehören zur Praxis. Das funktioniert auch deshalb so gut, weil die Verräter oft aus den eigenen Reihen kommen: Der Datenklau geht in knapp einem Viertel der Fälle von Mitarbeitern oder ehemaligen Angestellten aus.

Gern gewählter Angriffspunkt ist das IT-System eines Betriebs: Um an Informationen zu kommen, schleusen Industriespitzel Spionageprogramme ein oder fangen Tastatureingaben mit einem sogenannten Key Logger ab, einem kleinen Gerät, das zwischen Tastatur und PC angebracht wird und sämtliche Tastenanschläge des Nutzers protokolliert. Einen Komplizen für die Installation zu finden, ist für die Spione meist nicht schwer. Sie bieten viel Geld für die Mittäterschaft an: "Da bekommt die Reinigungskraft 5000 Euro dafür, dass sie in einem unbeobachteten Moment den Key Logger anschließt", gibt Experte Schaaf ein Beispiel. Ein Mitarbeiter, der sich beim Hausbau verkalkuliert hat, oder ein Praktikant mit teurem Hobby kann genauso zum Verbündeten werden wie ein Angestellter, der sich über die entgangene Beförderung ärgert: "Es ist die Kunst von Industriespionen, genau diese menschlichen Schwachstellen zu finden", sagt Schaaf.

Besonders dreiste Spitzel verschaffen sich den Zugang zu internen Daten sogar über Geschenke: So bekam kürzlich ein Vorstand einer deutschen Pharma-Firma einen edlen USB-Speicher mit Goldeinfassung von einem chinesischen Geschäftspartner überreicht. Auf dem Speicher fand der hauseigene IT-Experte ein Spionageprogramm: "Wäre das Gerät angeschlossen worden, wäre der komplette Inhalt des Computers nach China gemailt worden", erklärt Corporate-Trust-Geschäftsführer Schaaf.

Eine beliebte Methode sei auch, sich auf Kontaktanzeigen von Sekretärinnen zu melden oder auf Fachmessen als vermeintlicher Kollege mit den Entwicklungsingenieuren zu fachsimpeln, verrät Klaus-Dieter Matschke, Inhaber der Frankfurter Sicherheitsberatung KDM: "Irgendwo bekommen Sie fast jeden Menschen zu fassen." Und wenn kein Mitarbeiter sensible Daten ausplaudern möchte, stehlen geheimdienstlich geschulte Spione Laptops und Firmenunterlagen aus Hotelzimmern oder funktionieren Mobiltelefone zu Abhörgeräten um.

Absoluten Schutz gegen Betriebsspione gibt es nicht. Wer aber ein paar Vorkehrungen trifft, kann das Risiko beträchtlich senken: "Geschäftsreisende sollten wichtige Daten nicht auf ihrem Laptop speichern, sondern auf verschlüsselten USB-Speichern oder DVDs stets mit sich führen", rät Andrea Berner vom Hamburger Verfassungsschutz. Außerdem sollten sich Firmen ein Schutzkonzept für ihr Know-How überlegen. Dazu gehören nicht nur Sicherungsmaßnahmen für Telefone und Computer. Damit Mitarbeiter fragwürdige Kontakte überhaupt richtig einordnen können, müssen sie für die Tricks der Industriespione sensibilisiert werden und genau wissen, welche Interna sie keinesfalls ausplaudern dürfen. Sicherheitsexperte Schaaf empfiehlt, klare Sicherheitsregeln in den Arbeitsverträgen zu verankern: "Zum Beispiel interne Unterlagen nach Arbeitsende wegzusperrern und Passwörter nicht auf einem Zettel in der Ablage zu verwahren."

Außerdem rät er, einen abhörsicheren Raum zu schaffen und das Firmengebäude regelmäßig nach Wanzen durchsuchen zu lassen. Denn die nötige Technik für gezielte Lausangriffe ist dank gut bestückter Spionage-Läden für jedermann einfach zu beschaffen.

Link zum Artikel: <http://www.handelsblatt.com/betriebsspione-nehmen-mittelstaendler-ins-visier;2389456>

